POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) E LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

SUMÁRIO

1 INTRODUÇÃO

A Política de Segurança da Informação é necessária para implementar medidas e reduzir os riscos de acordo com as necessidades do Novo Hospital Santa Tereza.

Submeter-se a riscos é a capacidade de produzir perdas reais e mensuráveis de dados de uma instituição.

> Desde o surgimento da internet e consequentemente a unificação da rede mundial, as organizações e seus sistemas de informações e redes se deparam frequentemente com constantes e crescentes ameaças como: invasão, *hackers*, vírus, *spam*, espionagem, vandalismo, etc. A Segurança de Informações protege as informações por meio de normas, políticas, práticas, procedimentos, conscientização, treinamentos, estruturas e softwares, agindo diretamente sobre essas ameaças. (NBR ISO/IEC 17799:2000, pág. VI).

São atributos da Segurança da Informação:

Confidencialidade

Garantia de que o acesso à informação é restrito a pessoas autorizadas;

INTEGRIDADE

Está relacionado à segurança que os dados não foram modificados por pessoas não autorizadas;

DISPONIBILIDADE

Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos necessários sempre que for preciso;

AUTENTICIDADE

Está associada à identificação de um usuário ou computador. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos**.**

As normas descritas no decorrer da política devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas, considerando-se o tempo hábil para que eventuais providências sejam tomadas. A política de segurança da informação também segue a LGPD: Lei Geral de Proteção de Dados.

Tais normas são fornecidas, a título de orientação aos funcionários e demais envolvidos. Em caso de dúvida o funcionário ou outros parceiros deverão procurar a comissão de PSI visando esclarecimentos. As penalidades sofridas pelos usuários serão registradas em sua ficha funcional.

2 OBJETIVOS

São objetos da Política de Segurança, os serviços e recursos colocados à disposição dos funcionários e parceiros do Novo Hospital Santa Tereza, tais como: Computadores, correio eletrônico, Internet, informações armazenadas em diretórios da rede e sistemas de aplicação.

Onde se destacam as normas e procedimentos de utilização de recursos tecnológicos o objetivo é garantir que os recursos de informática e a informação serão utilizados de maneira adequada. Garantir a **informação como bem essencial do Hospital, respeitando sua confidencialidade, assegurando sua continuidade e a usando de maneira ética.**

> A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente. (NBR ISO/IEC 17799, setembro 2001).

Definem-se como *softwares*, todo e qualquer programa instalado nos computadores do Hospital, seja por tempo determinado ou não, independentemente de sua finalidade e/ou setor no qual estará sendo utilizado;

Definem-se como serviços relacionados, todo e qualquer serviço relacionado a cabeamento (ponto de rede), manutenção, consultoria ou assessoria nos equipamentos ou *softwares* do Hospital;

São considerados recursos computacionais: conjunto formado por um gabinete CPU, monitor, teclado, mouse e sistema operacional; *notebooks*; celulares; impressoras; copiadoras; *softwares*; internet; intranet; correio eletrônico (@ivirmond.com.br e/ou @novohst.com.br) e sistemas em geral como o Sistema de Gestão do Hospital: SPData e o GLPi (sigla: francês: *Gestionnaire Libre de Parc Informatique*, ou "Gestor de Equipamentos de TI de Código Aberto", em português) é um sistema de código aberto para Gerenciamento de Ativos de TI, rastreamento de problemas e central de serviços.

3 APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Política da Segurança da Informação do NOVO HOSPITAL SANTA TEREZA deverão ser aprovados e revisados. Assinados conforme anexo: 17.1

4 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os funcionários e colaboradores do NOVO HOSPITAL SANTA TEREZA e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento. Está disponibilizada na página do Novo Hospital Santa Tereza, www.novohst.com.br > área restrita, acessível utilizando computadores da rede do hospital.

5 DIRETORIAS, GERÊNCIAS E COORDENAÇÕES

Cabem às Diretorias, Gerências e Coordenações:

Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

Assegurar que suas equipes possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

Redigir os Procedimentos de Segurança da Informações relacionadas às suas áreas, mantendo-os atualizados; e

Comunicar imediatamente eventuais casos de violação de segurança da informação à área de Gestão de Segurança da Informação para a Comissão da PSI que é a responsável pela Gestão de Segurança da Informação.

6 CABE À ÁREA DE RECURSOS HUMANOS (RH) e DEPARTAMENTO PESSOAL (DP)

No ato da contratação, encaminhar o funcionário ou estagiário para o setor de Tecnologia da Informação para colher a assinatura dos termos, quantos cabíveis, Termo de Responsabilidade e de Utilização de Recursos Computacionais e do Termo de Responsabilidade de Utilização do Prontuário Eletrônico do Paciente (PEP) SPDATA, a TI deverá arquivar assinado e disponibilizar quando RH, DP e administração quando necessitarem.

Repassar para a TI as informações sobre funcionários desligados, imediatamente após assinatura do termo de rescisão de contrato, para controle e bloqueio de acessos;

Apoiar, mediante ações de treinamento e conscientização, as ações e programas de promoção do cumprimento e de mitigação de violações a esta política;

Registrar na ficha funcional do respectivo funcionário, as penalidades sofridas, pelo não cumprimento da Política de Segurança da Informação;

Atualizar no CNES (Cadastro Nacional de Estabelecimentos de Saúde) do hospital, as informações do funcionário como inclusão (novas contratações) e exclusão (demissões).

7 DEVERES CORRESPONDENTES E COMPROMISSOS DOS FUNCIONÁRIOS DO NOVO HOSPITAL SANTA TEREZA:

Fazer uso dos recursos computacionais para trabalhos de interesse exclusivo do Hospital;

Acessar a Intranet e a Internet, respeitando a política do HOSPITAL;

Fazer uso do telefone do hospital para tratar de assuntos relacionados ao trabalho;

Zelar por toda e qualquer informação armazenada na rede, contra alteração, destruição, divulgação, cópia e acessos não autorizados;

Quando funcionário e setor possuir conta de correio eletrônico com a extensão do domínio da empresa (@ivirmond.com.br ou @novohst.com.br), fazer uso para a instituição e não uso pessoal, é vetado o uso a outras contas de e-mail para tratar de assuntos relacionados ao hospital, como Gmail, Hotmail etc.

Mensagens de correio eletrônico são consideradas correspondências oficiais. Assim sendo, recomenda-se a identificação do usuário emitente, mediante inserção de informações ao final do texto, com a sua assinatura padrão (solicitar assinatura personalizada para o setor de TI) contendo as seguintes informações:

-Nome do remetente completo;
-Cargo;
-Setor;
-Telefone;
-E-mail

Jamais executar arquivos anexados nos e-mails com extensões *.eme, .com, .bat, .vbs, .scr, .exe;* sendo que estes devem ser eliminados imediatamente ou informado setor de TI para análise.

O setor de Tecnologia da Informação (TI) disponibiliza um sistema para registro de solicitações e incidentes, onde deverão ser registrados os chamados GLPI (http://192.168.0.251/glpi).

Quando for necessária a mudança de local de um computador ou qualquer outro recurso computacional para qualquer local diferente, é dever do funcionário solicitar a equipe de TI para realizar a mudança, pela questão patrimonial e configurações de rede evitando também queima do equipamento. Solicitar através do GLPI.

A responsabilidade pela guarda e execução das cópias de segurança, das informações armazenadas **nas estações de trabalho (computador),** será do usuário da estação de trabalho. Não será realizado, pela área de Tecnologia, *backup* ou cópia de segurança de nenhuma informação ou arquivo armazenado nessas estações.

Quando necessário, o proprietário da Informação deve solicitar formalmente à área de Tecnologia, a cópia e a restauração da cópia de segurança da informação, armazenada nas estações de trabalho.

Para a equipe de enfermagem, armazenar arquivos e documentos, existe uma pasta compartilhada na rede que chamamos de “Enfermagem para todos” (\\192.168.0.251\Enfermagem) essa pasta está segura e sendo realizados backups diários.

8 PROIBIÇÕES

Não fazer uso da rede para molestar, ameaçar ou ofender os usuários, colegas de trabalho, pacientes, acompanhantes ou terceiros, por quaisquer meios, sejam textos, imagens, fotos, vídeos ou correios eletrônicos;

É vedado ao funcionário, abrir o gabinete da estação de trabalho (computador do setor) e instalar dispositivos de *hardware*, por quaisquer motivos;

Não instalar qualquer sistema operacional ou *softwares*, inclusive livres ou gratuitos, na estação de trabalho, sem autorização prévia do setor de TI;

Fazer cópia, para uso externo, de *softwares* adquiridos pelo Novo Hospital Santa Tereza;

Compartilhar a unidade do disco rígido (raiz) entre usuários;

Danificar ou remover a identificação dos equipamentos, como as etiquetas, lacres ou placas de patrimônio;

Realizar conexões de rede, bem como conexões de recursos computacionais pessoais na rede administrativa;

Realizar a transmissão ou posse de informações que impliquem violação de direitos autorais (pirataria) ou de propriedade da informação;

Utilizar servidores e computadores do NOVO HOSPITAL SANTA TEREZA para armazenamento de arquivos pessoais como fotos, músicas e outras informações pessoais;

Burlar ou tentar burlar os dispositivos de segurança da rede;

Revelar a terceiros sua identificação de usuário e senha de acesso à rede ou qualquer sistema do Hospital como o sistema da SPData. Pois sua senha é pessoal e intransferível.

Acessar ou navegar em sites que não sejam ligados ao desenvolvimento da atividade de trabalho;

Fazer *download* de arquivos executáveis ou de multimídia, mesmo que estejam compactados sem autorização prévia do setor de TI;

A instalação de equipamentos de rede sem fio (*Access Point*) sem autorização prévia do setor de TI;

Proibido fotografar e filmar pacientes e acompanhantes sem que tenham permissão dos mesmos. O mesmo vale para divulgações de imagens (fotos e vídeos) em redes sociais como exemplo: Facebook, Twitter e Instagram.

9 RECOMENDAÇÕES

Proteja sempre a sua senha. Quando encerrar as operações no SGH SPDATA, tenha o cuidado de sair do sistema;

Os acessos aos sistemas SPDATA somente poderão ser feitos, após o cadastramento de usuário e senha **pessoal**, pela equipe de TI do NOVO HOSPITAL SANTA TEREZA, não usar senha do colega;

O funcionário deverá solicitar ao setor de TI a troca de sua senha SPDATA E EMAIL, caso considere conveniente, por motivo de segurança.

Qualquer ocorrência (quebra, falha, mau funcionamento, incidente, desaparecimento) relacionada aos equipamentos de informática deverá ser informada imediatamente à Área de Tecnologia.

Em razão do avanço da tecnologia e de aparelhos de última geração, um grande número de funcionários tem acesso a smartphones e consequentemente às redes sociais e aplicativos de comunicação como WhatsApp. Portanto é regra interna de cada setor e departamento o uso da ferramenta durante o horário de expediente.

10 CABE AO SETOR DE TÉCNOLOGIA DA INFORMAÇÃO

Instalar *software* de acesso remoto nas estações de trabalho com o intuito de aperfeiçoar os processos de monitoramento e atendimento dos usuários;

Remover *softwares* instalados que não condizem com as atividades institucionais;

Executar programas de inventário, a fim de identificar *softwares* sem licenciamento ou danosos à rede;

Criar regras de bloqueio de sites que possuam conteúdos indevidos a fim de gerenciar o uso da ferramenta;

Excluir automaticamente mensagens dos servidores com conteúdo indevidos ou que possuam códigos maliciosos;

Limitar o uso da banda de internet e caixa postal dos usuários, de acordo com as necessidades do NOVO HOSPITAL SANTA TEREZA;

Interromper os serviços de internet e correio eletrônico corporativo quando necessário;

Solicitar, quando necessário, a troca de senhas de rede, de sistemas, de sites e de Correio Eletrônico e exigir senhas complexas;

Excluir ou tornar inativa, as contas SPDATA, Spark e de Correio Eletrônico dos funcionários desligados do NOVO HOSPITAL SANTA TEREZA;

Toda solicitação de equipamentos, *softwares* ou serviços deverá ser feita ao Setor de Tecnologia da Informação (TI) por meio de sistema de chamados GLPI;

Ao realizar mudança de um computado ou qualquer outro recurso computacional de um local para outro, comunicar o responsável pelo patrimônio (controladoria), editar os ativos no GLPI, informando a descrição do equipamento, o número de patrimônio, de onde foi retirado e onde foi reinstalado o mesmo;

Ao realizar mudança de um computador para qualquer outro local, deve existir identificação na tomada de rede e no posicionamento dos cabos no switch/patch panel, possuir notas do *Internet Protocol* (endereço IP do computador) e em qual porta do *switch* se encontra (gerenciar adequadamente a rede). Tanto física quanto no sistema para gerenciar a rede: *BrazilFW*;

Todos os servidores e estações de trabalho serão protegidos por *software* de antivírus, devendo estar sempre ativo e atualizado, seguindo as configurações definidas pela área de Tecnologia, não podendo ser removido pelo usuário em nenhuma hipótese.

11 QUANTO À REALIZAÇÃO DE *BACKUP*, CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS:

Entende-se por *backup* as operações de cópia feitas diariamente, com prazo curto de vida, para garantir o retorno de falhas no sistema;

Entende-se por cópias de segurança as operações de cópia feitas em períodos de tempo mais longo.

O setor de Tecnologia da Informação é responsável por efetuar as operações de *backup*, cópia de segurança e restauração das informações armazenadas **nos servidores da rede** do NOVO HOSPITAL SANTA TEREZA; bem como banco de dados do sistema SPDATA, backups diários.

Conferir e realizar backups diários da pasta “enfermagem para todos”.

Realização de backup semanal do computador do departamento pessoal em HD Externo.

Sistemas do SUS como CCIH, SIA SUS e BPA a TI irá realizar mensalmente uma cópia de segurança.

Sistemas da controladoria deverão ser armazenados pelo setor de controladoria na pasta da rede compartilhada entre o setor, essa pasta no servidor a TI estará realizando backups diários.

Sistema da tesouraria TAG Soft a TI deverá realizar um backup mensal.

12 QUANTO AO USO DAS IMPRESSORAS E COPIADORAS

O serviço de impressão é prestado por empresa terceirizada. E podem ser geradas auditorias.

Cabe ao setor de informática definir que tipo de impressora cada departamento e setor devem utilizar;

As solicitações de reparo no equipamento e troca de periféricos devem ser realizadas por meio do sistema de chamados do NOVO HOSPITAL SANTA TEREZA;

O setor, departamento, funcionário que quebrar ou danificar uma impressora ou copiadora, deverá arcar com a despesa do equipamento.

13 QUANTO AO ACESSO A REDE E SEUS SERVIÇOS

O acesso ao ambiente informatizado deverá ser concedido unicamente por meio de identificação (endereço MAC);

O acesso à rede será válido por tempo determinado, enquanto vigorar o contrato de trabalho do funcionário ou do prestador de serviço;

Quando for constatado a necessidade de acesso à rede por terceiros, o mesmo poderá ser solicitado pelo responsável do setor ou departamento. O acesso será concedido apenas se aprovado pelo setor de TI após análise;

É dever do funcionário (usuário) a proteção de suas credenciais de acesso a sistemas de informação. O detentor do usuário e senha deverá assumir a responsabilidade pela guarda, descrição ou sigilo das operações decorrentes do seu uso. Recomenda-se a troca de senha a cada noventa dias.

A utilização do acesso à Internet no Hospital deve estar prioritariamente relacionada às tarefas desempenhadas pelo funcionário. Uso pessoal de ordem eventual é permitido, desde que seja fora do horário de trabalho para não consumir recursos significativos de tempo ou interferir na produtividade pessoal. Será monitorado o uso da internet em todos os computadores e colaboradores e computadores, no monitoramento será visualizado o endereço data e hora web (http e https) que foi acessado e entregue ao seu supervisor.

É vetado o acesso a sites de conteúdo criminoso, de apostas ou pornografia. A TI tentará restringir os acessos a sites que considerar alheios aos objetivos do Hospital e monitorar consultas de usuários, com o objetivo de garantir segurança e adequação no uso deste recurso;

O acesso a serviços como Internet, sites específicos, e outros devem ser solicitados formalmente pelo responsável da área interessada à Área de Tecnologia, justificando o pedido;

Caso seja necessário o compartilhamento de arquivos entre usuários, este poderá ser solicitado ao setor de TI;

Não é recomendado, **mas em casos excepcionais** será permitido aos usuários proprietários de *notebook* pessoal o acesso à rede, desde que sejam autorizados pelo setor de TI. A permissão de uso de *notebooks* e demais computadores portáteis pessoais será concedida após o

cumprimento de todas as normas de segurança, ou seja, é obrigatório que o Sistema Operacional e o *software* de antivírus estejam atualizados devendo o setor de TI do NOVO HOSPITAL SANTA TEREZA verificar. E a TI do hospital se isenta de qualquer defeito, desconfigurações de computadores e notebooks pessoais utilizados no hospital.

14 QUANTO À INSTALAÇÃO E UTILIZAÇÃO DE *SOFTWARES*:

A utilização de *softwares* será disponibilizada mediante os seguintes procedimentos:

Validação dos requisitos técnicos definidos pela área de tecnologia;

Disponibilidade e aquisição de licença de *software*;

Instalação, pela área de tecnologia, do *software* adquirido;

Os equipamentos de informática funcionarão somente com *softwares* regularmente adquiridos e licenciados junto a seus fornecedores ou representantes, ou ainda, aqueles desenvolvidos pelo quadro de funcionários do hospital;

A área de Tecnologia, periodicamente, efetuará auditoria nas estações de trabalho, objetivando manter o padrão de *softwares* nos equipamentos;

A instalação de *softwares* sobre os quais o NOVO HOSPITAL SANTA TEREZA não detenha direitos e que visem atender interesses de parcerias com as quais mantenha acordo operacional, deverá ser precedida de contrato que preserve o NOVO HOSPITAL SANTA TEREZA de qualquer ônus;

15 DISPOSIÇÕES GERAIS

Todos os funcionários deverão assinar o termo de responsabilidade de uso dos recursos computacionais, declarando pleno conhecimento dos termos desse regulamento;

O termo de responsabilidade de uso dos recursos computacional preenchido e assinado deverá ser arquivado no setor de tecnologia da informação;

Todas as regras estabelecidas neste regulamento se aplicam também aos prestadores de serviço;

É de inteira responsabilidade do funcionário, o uso de qualquer recurso computacional que não seja patrimônio do NOVO HOSPITAL SANTA TEREZA. Portanto, qualquer desgaste ou dano de

equipamentos, decorrentes do seu uso nas dependências do Hospital, será da sua inteira responsabilidade.

16 REFERÊNCIAS

- NBR ISO/IEC 17799:2000.

- ISO 27001

> A ISO 27001 é uma norma internacional de segurança da informação. Certifica as organizações em relação aos sistemas gerenciais de segurança da informação. Nasceu no governo britânico, através da norma ISO 17799, que por sua vez veio da norma BS 7799.

- Unimed Guarapuava PR.

- SBIS – Sociedade Brasileira de Informática em Saúde.

- LGPD Brasil.com.br (https://www.lgpdbrasil.com.br/)

17 ANEXOS

17.1 Aprovação da Política de Segurança da Informação do Novo Hospital Santa Tereza e Comissão PSI

Elaborado por:

Documento Original Assinado
data 05/07/2021

_____

· Andressa Bittar Kava
Gerente de TI

Integrante da Comissão PSI e LGPD

Revisado e Aprovado por:

_____

· Marlon Mallassa
Diretor de Planejamento

_____

· Monique Mallassa
Diretora de Assistência e Qualidade

De acordo:

_____

· Creagair Aparecida de Oliveira
Diretora Administrativa

Documento Original Assinado
data 07/07/2021

_____

· Andre Luiz Stempinhaki
Auxiliar Técnico de Informática
Integrante da Comissão PSI

Documento Original Assinado
data 08/07/2021

_____

· Vinicios Hansberto da Fonseca
Técnico de Informática
Integrante da Comissão PSI

17.2 Termo de Responsabilidade e de Utilização de Recursos Computacionais e/ou Utilização do Prontuário Eletrônico do Paciente (PEP) SPDATA

Política de Segurança da Informação

TERMO DE RESPONSABILIDADE E DE UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS e/ou USO DO PEP SPDATA

(todos os funcionários e médicos deverão assinar)

Guarapuava, 1 de setembro de 2023.

Eu, _____, RG ou CPF:_____, Setor/Departamento:_____, declaro estar ciente dos termos da política de segurança da informação do hospital, autorizo o monitoramento das atividades computacionais, do uso do sistema de gestão hospitalar (SGH) e o uso do telefone do NOVO HOSPITAL SANTA TEREZA; também comprometo-me com zelo dos computadores e impressoras do hospital, estando ciente dos meus direitos, obrigações e deveres para com este hospital.

O (SGH) SPDATA é o sistema que o NOVO HOSPITAL SANTA TEREZA utiliza para manipulação de dados e geração de informações para benefícios e tomadas de decisão na instituição. Para os serviços como e-mail, uso do SGH recebo um *login* e senha **pessoal** para acesso; dessa forma, comprometo-me a fazer uso das senhas, de forma segura e confidencial, zelando por sua guarda e confidencialidade, declarando-me ciente de que não poderei transferir, ceder ou emprestar, a qualquer título, senhas, pois são de caráter pessoal e intransferível.

(Quando registrado no CRM) Estou ciente de que as prescrições só serão aceitas se forem cadastradas eletronicamente no SGH, só assim garanto a medicação para meus pacientes.

Estou informado (a) que o NOVO HOSPITAL SANTA TEREZA mantém -em arquivo digital- a identificação dos funcionários que utilizam à rede e os endereços que estes acessaram na Internet, para resposta as diretorias legais, se assim o exigirem.

_____

Assinatura Funcionário (a).

registrado com nº do conselho: _____ (quando houver COREN, CRM, CRF, CREFITO, etc)